Information security policy

Version: 1.0

Approval Date: July 27, 2026

At **Quantori**, we understand that security, data integrity, and privacy are paramount—especially given our work in advanced software engineering, life sciences, and healthcare IT solutions. We are deeply committed to protecting the data entrusted to us by our clients, partners, and website visitors.

1. Compliance and Certifications

Quantori maintains rigorous information security management systems to protect client data and intellectual property. Our security posture is independently audited and validated by accredited third parties:

- **SOC 2 Type II:** Our controls and operational processes regarding security, and confidentiality undergo regular independent third-party audits.
- **ISO/IEC 27001:2022:** We are certified against the globally recognized standard for information security management, ensuring continuous, comprehensive risk management.

Note: Copies of our current SOC 2 Type II report and ISO 27001:2022 certificate are available to clients and partners under a Non-Disclosure Agreement (NDA) upon request by contacting compliance@quantori.com*.*

2. Data Protection and Encryption

- **Data in Transit:** All traffic connecting to Quantori web properties and digital platforms is encrypted using industry-standard Transport Layer Security (TLS 1.2 or higher) to safeguard information against interception.
- **Data at Rest:** Sensitive data repositories and corporate assets are protected using robust encryption protocols and strict access controls.

3. Secure Engineering and Development

As a trusted technology partner, Quantori incorporates security into every stage of our digital lifecycle:

- **Secure Coding Practices:** Our development teams adhere to rigorous engineering standards designed to mitigate common web vulnerabilities (aligned with OWASP Top 10 guidelines).

- **Environment Isolation:** Development, testing, and production environments are strictly segregated to maintain system integrity and stability.

4. Access Control and Governance

- We adhere to the Principle of Least Privilege, ensuring that only authorized personnel have access to specific administrative systems and data repositories.
- Multi-factor authentication (MFA) and strict credential management policies are enforced across our operational environments.

5. Vulnerability Management

We maintain a proactive approach to identifying and addressing potential security gaps:

- Regular vulnerability assessments and security reviews are performed on our public-facing web applications.
- We actively monitor and apply patches to underlying frameworks, dependencies, and infrastructure components.

6. Reporting a Security Vulnerability

Quantori values the security community and appreciates responsible disclosure. If you believe you have discovered a security vulnerability on any Quantori website or digital asset, please report it to our security team.

- **Email:** security@quantori.com
- **What to include:** A detailed description of the vulnerability, steps to reproduce, and any relevant proof-of-concept information.

We pledge to work with researchers to investigate and resolve valid reports promptly.